VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts P02106WO.1P	**WEITERES VORGEHEN** siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE 03/04190	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 19.12.2003	Prioritätsdatum *(Tag/Monat/Jahr)* 08.01.2003
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/32		
Anmelder DEUTSCHE TELEKOM AG et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 3 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Bescheids
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Regel 66.2 a)ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
28.07.2004	03.12.2004
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Cretaine, P Tel. +49 89 2399-8828

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE 03/04190

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung *(Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17))*:

Beschreibung, Seiten

1-13 in der ursprünglich eingereichten Fassung

Ansprüche, Nr.

1-8 eingegangen am 17.11.2004 mit Schreiben vom 16.11.2004

Zeichnungen, Blätter

1/1 in der ursprünglich eingereichten Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um:

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).

   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:

   ☒ Ansprüche, Nr.: 9-10

   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen.)

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-8
	Nein:	Ansprüche	
Erfinderische Tätigkeit (IS)	Ja:	Ansprüche	1-8
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (IA)	Ja:	Ansprüche:	1-8
	Nein:	Ansprüche:	

2. Unterlagen und Erklärungen:

   siehe Beiblatt

Zu Punkt V

Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Es wird auf die folgende Dokumente verwiesen:

   D1 = DE 198 45 199 A (MAZ MIKROELEKTRONIK ANWENDUNGS) 6. April 2000 (2000-04-06)

   D2 = US 2002/169970 A1 (CANDELORE BRANT L) 14. November 2002 (2002-11-14)

2. Der Anmeldungsgegenstand betrifft ein Verfahren (**Anspruch 1**) und ein System (**Anspruch 7**) zur Bereitstellung eines Zeitstempels durch ein manipulationssicheres Zeitsignal in einem Telekommunikationsnetzwerk, sowie die Verwendung (Anspruch 5) des Verfahrens bei der Übermittlung von Daten zwischen Netzwerteilnehmern.

3. **Stand der Technik:**

   Den nächstliegenden Stand der Technik bildet das Dokument D1. Aus D1 ist ein Verfahren gemäß dem Oberbegriff des Anspruchs 1 bekannt, wobei ein amtlich anerkanntes Zeitsignal von einem Mobil-Netzbetreiber empfangen und verschlüsselt wird und über das Mobiltelekommunikationsnetzwerk an Netzwerteilnehmern übermittelt und entschlüsselt wird.

4. **Neuheit:**

   Der Gegenstand der unabhängigen Ansprüche 1 und 7 unterscheidet sich daher von dem bekannten Verfahren dadurch, daß:
   - Verschlüsselung und Entschlüsselung mit demselben Schlüssel erfolgt
   - bei dem Zentralsystem und bei den Netzwerkteilnehmer synchron arbeitenden Uhrsysteme vorhanden sind, die zur Erzeugung eines sich zeitlich synchron ändernden Schlüssels dienen.

Der Gegenstand des Anspruchs 1 (und des Anspruchs 7) ist somit neu (Artikel 33(2) PCT).

5. **Erfinderische Tätigkeit:**

Die mit der vorliegenden Erfindung zu lösende Aufgabe kann somit darin gesehen werden, daß die Verschlüsselung des Zeitsignals sicherer gegen Manipulationen wird.

Die in den Ansprüchen 1 und 7 der vorliegenden Anmeldung für diese Aufgabe vorgeschlagene Lösung beruht aus den folgenden Gründen auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT):

In D1 erfolgt die Verschlüsselung des Zeitsignals nicht beim Zentralsystem sondern beim Mobil-Netztreiber; eine Manipulation des amtlich anerkanntes Zeitsignals ist deshalb zwischen dem Zentralsystem und dem Mobilnetz möglich. Die Verschlüsselung in D1 basiert dazu auf der Technologie des Netzbetreibers und keine zeitliche Änderung des symmetrisches Schlüssels durch synchron arbeitenden Uhrsysteme ist vorgeschlagen.

D2 beschreibt ein ähnliches System wie D1 für einen "content players" Netzwerk. Auch hier erfolgt die Verschlüsselung des Zeitsignals nicht mit einem zeitlich ändernden symmetrischen Schlüssel.

Die Ansprüche 2-6 und 8 sind vom Anspruch 1 oder 7 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit und erfinderische Tätigkeit.

6. **Bemerkungen:**

Die in den Ansprüchen 1 und 7 benutzte Ausdruck "insbesondere" läßt den Leser über das Vorhandensein des betreffenden technischen Merkmals im Schutzbereich der Ansprüchen 1 und 7 im Ungewissen.

Telekom P-02106 16.11.2004

Patentansprüche

1. Verfahren zur Bereitstellung eines Zeitstempels durch ein manipulationssicheres Zeitsignal (5, 10) über ein Telekommunikationsnetzwerk (2), wobei ein Netzwerkteilnehmer (1a, 1b, ..., 1e) von einem Zentralsystem (3) ein insbesondere amtlich anerkanntes Zeitsignal (5, 10) anfordert, welches vom Zentralsystem (3) mit wenigstens einem Schlüssel verschlüsselt wird, nach der Verschlüsselung über das Telekommunikationsnetzwerk (2) an den Netzwerkteilnehmer (1a, 1b, ..., 1e) übermittelt und von diesem entschlüsselt wird, **dadurch gekennzeichnet, dass** Verschlüsselung und Entschlüsselung mit demselben/denselben Schlüssel/n erfolgt, wofür beim Netzwerkteilnehmer (1a, 1b, ..., 1e) und beim insbesondere zertifizierten Zentralsystem (3) je wenigstens ein Uhrsystem (4a, 4b, ..., 4e, 6a, 6b,..., 6e) vorgesehen ist, wobei je zwei Uhrsysteme (4a - 6a, 4b - 6b,..., 4e - 6e) einander und dem Netzwerkteilnehmer (1a, 1b, ..., 1e) zugeordnet sind und synchron arbeiten zur Erzeugung eines sich zeitlich synchron ändernden Schlüssels.

2. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** das Zentralsystem (3) bei der Abfrage eines Zeitsignales (5,10) durch einen Netzwerkteilnehmer (1a, 1b, ..., 1e) ein diesem zugeordnetes Uhrsystem (4a, 4b, ..., 4e) anhand einer übermittelten Kennung, insbesondere der Netzwerkadresse des Netzwerkteilnehmers (1a, 1b, ..., 1e), ermittelt und mittels einem von dem zugeordneten Uhrsystem (4a, 4b, ..., 4e) erzeugten Schlüssel und/oder der Kennung das Zeitsignal (5,10) verschlüsselt und übersendet.

3. Verfahren nach einem der verherigen Ansprüche, **dadurch gekennzeichnet, dass** ein Zentralsystem (3) beim zweiten Netzwerkteilnehmer vorgesehen ist.

4. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** das Zentralsystem (3) eine Empfangsquittierung, insbesondere mit einem Zeitsignal (5,10) an den ersten Netzwerkteilnehmer (1a, 1b, ..., 1e) zurücksendet.

5. Verwendung eines Verfahrens nach einem der vorherigen Ansprüche zur Übermittlung von Daten mit einem manipulationssicheren Zeitstempel über ein Telekommunikationsnetzwerk (2) von einem ersten Netzwerkteilnehmer zu einem zweiten Netzwerkteilnehmer **dadurch gekennzeichnet, dass** die Daten von dem ersten Netzwerkteilnehmer zusammen mit einem Zeitsignal an den zweiten Netzwerkteilnehmer direkt oder indirekt über das Zentralsystem (3) übermittelt werden.

6. Verwendung nach Anspruch 6, **dadurch gekennzeichnet, dass** die Daten und/oder das Zeitsignal bei der Übermittlung vom ersten Netzwerkteilnehmer (1a, 1b, ..., 1e) verschlüsselt werden, insbesondere mit dem beim Zentralsystem (3) und ersten Netzwerkteilnehmer (1a, 1b, ..., 1e) vorliegenden Schlüssel und/oder einer Kennung des ersten Netzwerkteilnehmers (1a, 1b, ..., 1e).

7. System zur Erzeugung eines manipulationssicheren Zeitstempels in netzwerkbasierten Kommunikationssystemen **dadurch gekennzeichnet, dass** es ein Zentralsystem (3) und wenigstens je ein Uhrsystem (4a, 4b, ..., 4e, 6a, 6b,..., 6e) auf seiten eines Netzwerkteilnehmers (1a, 1b, ..., 1e) und des Zentralsystems (3) umfasst, wobei je zwei Uhrsysteme (4a - 6a, 4b - 6b,..., 4e - 6e) einander und dem Netzwerkteilnehmer (1a, 1b, ..., 1e) zugeordnet sind und synchron arbeiten zur Erzeugung eines sich insbesondere in Zeitintervallen ändernden Schlüssels mittels dem ein insbesondere amtlich anerkanntes Zeitsignal (5,10) im Zentralsystem (3)

verschlüsselbar und nach Übersendung an den Netzwerkteilnehmer (1a, 1b, ..., 1e) von diesem entschlüsselbar ist.

8. System nach Anspruch 7, **dadurch gekennzeichnet, dass** ein Zeitzeichensender (5) das Zentralsystem (3) bildet.